(USAO GAN 6/10) Search Warrant

United States District Court

NORTHERN DISTRICT OF GEORGIA

In the Matter of the Search of

28 Ivory Court, Hiram, Georgia, 30141

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

Case number: 4:20-MC-016

I, James Rives, depose and say under penalty of perjury:

I am a Special Agent of the Other and have reason to believe that on the property described as:

See Attachment A

in the Northern District of Georgia there is now concealed certain property, certain information, and certain data, namely,

See Attachment B,

which constitutes evidence of a crime, contraband, fruits of crime, or items illegally possessed, and property designed for use, intended for use, or used in committing a crime, concerning violations of Title 18, United States Code, Section(s) 2252(a)(4). The facts to support a finding of Probable Cause are as follows:

SEE ATTACHED AFFIDAVIT

Continued on attached sheet made a part hereof.

Sworn to me by telephone pursuant to Federal Rule of Criminal Procedure 4.1

Signature of Affiant

James Rives

April 30, 2020
Date

Cartersville, Georgia
City and States

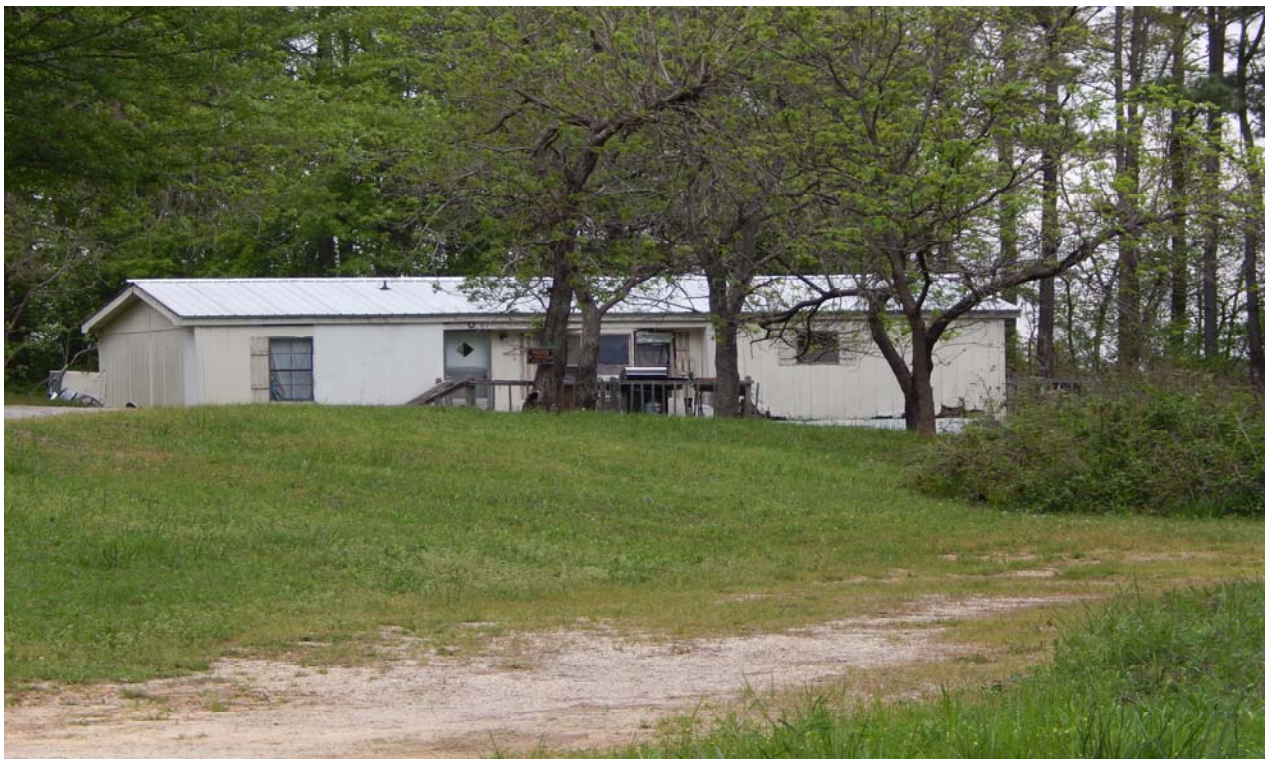
Name and Title of Judicial Officer

WALTER E. JOHNSON
UNITED STATES MAGISTRATE JUDGE

AUSA Laurel R. Boatright

ATTACHMENT A

The **SUBJECT PREMISES** is located at 28 Ivory Court, Hiram, Georgia 30141. The residence is described as a single-family white mobile home with white trim, roof and shutters. The front door is white and is located in the front of the mobile home.



ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

A. Evidence, Fruits, and Instrumentalities of the Subject Offense

The items to be seized from the **SUBJECT PREMISES** are the following evidence, fruits, and instrumentalities of violations of Title 18, United States Code Section 2252(a)(4) (the SUBJECT OFFENSE) described as follows:

1. Computers, storage media, and related electronic equipment used to access, transmit, or store information relating to the SUBJECT OFFENSE.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereafter, "COMPUTER"):

    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

    c. evidence of the lack of such malicious software;

    d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

    e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

    f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

    g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography and child erotica.

5. Records, information, and items relating to violation of the SUBJECT OFFENSE including

a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES including utility and telephone bills, mail envelopes, or addressed correspondence;

b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

c. Records and information relating to the identity or location of the persons suspected of violating the SUBJECT OFFENSE; and

d. Records and information relating to sexual exploitation of children, including correspondence, communications, and records that could assist in victim identification.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

B. Search and Seizure of Electronically Stored Information

The items to be seized from the **SUBJECT PREMISES** include any computer devices, storage media, and related electronic equipment that may contain or constitute fruits, evidence, and/or instrumentalities of the SUBJECT OFFENSE falling within the categories set forth in Section A above. In lieu of seizing any such computer devices, storage media, and related electronic equipment, this warrant also authorizes their copying for later review.

To facilitate this review, the items to be seized from the **SUBJECT PREMISES** also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices, storage media, and related electronic equipment, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.

2. Any items or records that may facilitate a forensic examination of any seized or copied computer devices, storage media, and related electronic equipment, including but not limited to any hardware or software manuals or other

information concerning the configuration of the seized or copied computer devices or storage media.

3. Any records or other items which evidence ownership, control, or use of, or access to any seized or copied computer devices, storage media, and related electronic equipment, including but not limited to sales receipts, warranties, bills for internet access, handwritten notes, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.

C. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (which may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Sections A and B of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary, to evaluate its contents and to locate all data responsive to the warrant.

I, James Rives, do hereby depose and state under penalty of perjury:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Federal Rule of Criminal Procedure 41 for a search warrant for the property located at 28 Ivory Court, Hiram, Georgia, 30141 (the **SUBJECT PREMISES**), more particularly described in **Attachment A**. I request authorization to search for and seize the items enumerated in **Attachment B**, which constitute evidence, contraband, fruits and instrumentalities of violations of Title 18, United States Code, Section 2252(a)(4), which criminalizes the possession of child pornography.

2. I am a Special Agent (SA) of the United States Department of Homeland Security (DHS) Immigration & Customs Enforcement (ICE), Homeland Security Investigations (HSI) assigned to the Dalton, Georgia office, and have been employed by HSI since April 2007.

3. I have completed the Criminal Investigator Training Program and HSI Special Agent Training at the Federal Law Enforcement Training Center in Glynco, Georgia. Prior to being employed with ICE, I served as a police officer for seven years with the Alpharetta, Georgia Police Department. During my last two years with the Alpharetta Police Department, I served on a Federal Gang Task Force. I received training and have actual experience related to federal criminal procedures, federal statutes, and DHS regulations.

4. As a Special Agent, I am responsible for enforcing federal criminal statutes, including Title 18, United States Code, Sections 2252 and 2252A, the sexual exploitation

of children. I have received training and instruction in the investigation of child pornography offenses and have had the opportunity to conduct, coordinate, and participate in investigations related to the sexual exploitation of children. As part of my training and experience, I have reviewed images containing child pornography in a variety of formats (such as digital still images and video images) and media (such as videotapes and printed images).

5. The statements contained in this Affidavit are based on my personal observations, my training and experience, as well as information obtained from other agents and witnesses. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. Rather, I have set forth only the facts that I find necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252(a)(4)(B) (the possession of child pornography) will be found at the **SUBJECT PREMISES**. I, therefore, respectfully request that the attached warrant be issued authorizing the seizure and search of the items listed in **Attachment B**.

BACKGROUND ON SKYPE

6. Skype is a telecommunications application that specializes in providing video chat and voice calls between computers, tablets, mobile devices, the Xbox One console, and smartwatches over the Internet. Skype also provides instant messaging services. Users may transmit text, video, audio and images. Skype allows video conference calls.

7. Registered users of Skype are identified by a unique Skype ID and may be listed in the Skype directory under a Skype username. Skype allows these registered users to communicate through both instant messaging and voice chat. Voice chat allows telephone calls between pairs of users and conference calling and uses proprietary audio codec. Skype's text chat client allows group chats, emoticons, storing chat history, and editing of previous messages. The usual features familiar to instant messaging users—user profiles, online status indicators, and so on—are also included.

8. Skype subscribers obtain an account by registering with Skype. During the registration process, Skype asks subscribers to provide basic personal information and to select a username. During this process, Skype registers the date, time, internet protocol (IP) address,[1] and information related to the device used to complete the account registration. The username is the only unique identifier used by Skype.

CURRENT INVESTIGATION

9. On January 11, 2018, Daniel Yarbrough (a/k/a Ami Rain Dark) was the suspect of a child exploitation investigation in Polk County, Georgia, based on two (2) cyber tip reports from the National Center for Missing and Exploited Children (NCMEC). The cyber tips (20708780 & 20711116) were priority "E", which means that they were forwarded by an Electronic Service Provider (ESP). In this case, the ESP was a Dropbox account associated with the email address oniwabondark@yahoo.com. Upon

[1] An IP address is a series of four sets of digits separated by a decimal. The Internet Service Provider supplies the IP address to its customers, which is used to access the internet. The IP address identifies the physical location of the computer or electronic device that accessed the internet during the relevant period.

identifying Yarbrough as the user of the Dropbox account, the Polk County Police Department obtained arrest warrants for Yarbrough based on the images and videos identified from the Dropbox cyber tips. The arrest warrant was for 30 counts of possession of child pornography.

10. On January 11, 2018, Yarbrough was located at the residence of 28 Ivory Court, Hiram Georgia, 30141. A post-*Miranda* waiver interview with Yarbrough lead to Yarbrough admitting to uploading the child pornography. Yarbrough explained she viewed and collected child pornography because she wanted to see a child suffering and in pain much like what he was going through during her transition to becoming a female.[2]

11. On January 11, 2018, Yarbrough was arrested on a state warrant for 30 counts of possession of child pornography and transported to the Polk County Jail. Subsequently, Yarbrough was released on pretrial bond under certain conditions, including that she not violate state or federal law (including possession of child pornography).

12. In August 2019, HSI Special Agent (SA) Jeanne Pickard received Cyber Tipline reports 51563649 and 51563239 from NCMEC. The submitter to NCMEC of both reports was Microsoft Online Operations who reported the discovery of child pornography within peer to peer Skype Media Storage. According to report 51563649, the incident occurred on June 29, 2019, at 23:31:32 UTC from user "cutelilkittenbaby" at

[2] **D**uring the interview, Yarbrough requested to be called Ami Rain Dark and to be referred to as a female. Yarbrough has not had his name legally changed.

IP address 99.127.129.80. The file name was provided as well as the image of child pornography. Cyber Tipline report 51563239 reported the incident date of June 29, 2019, at 22:54:28 UTC from user "cutelilkittenbaby" at IP address 99.127.129.80. At that time, SA Pickard was unaware of the HSI Dalton investigation and initiated an investigation into the person responsible for downloading child pornography images through Skype.

13. During her investigation, SA Pickard discovered that IP address 99.127.129.80 resolves to AT&T. On August 22, 2019, HSI SA Pickard sent AT&T a subpoena for subscriber and customer information for IP address 99.127.129.80 dated June 29, 2019 at 22:54:28 UTC and June 29, 2019 at 23:31:32 UTC.

14. On August 29, 2019, subpoena results from AT&T t for subscriber and customer information related to IP address 99.127.129.80 on those dates and times revealed the following:

Name:	John Croker
Address:	28 Ivory Court Hiram, GA 30141
Phone Number:	678-294-7937

During the prior investigation, I learned that John Croker is Yarbrough's brother who resides at 97 Sycamore Street, Rockmart, Georgia. Croker is also being investigated for the possession of child pornography by HSI.

15. On September 26, 2019, SA Pickard searched the Paulding County Tax Assessor's website for the **SUBJECT PREMISES**, and learned the property is owned by Thomas E Croker, heirs of Johnny Croker.

16. On October 4, 2019, I served Daniel Yarbrough (a/k/a Ami Rain Dark) a target letter from the United States Attorney's Office informing her of the government's intent to bring formal criminal charges against her for the possession of child pornography. I served Yarbrough with the letter at the **SUBJECT PREMISES**. During the investigation, I learned the residence is owned by her father, Thomas Croker, and Yarbrough lives alone at the residence. Before arriving at the residence, I met with Yarbrough's mother at 97 Sycamore Street, Rockmart, Georgia, who also informed me that Yarbrough lives alone.

17. On January 22, 2020, I learned about the active investigation conducted by HSI Atlanta Special Agent (SA) Jeanne Pickard referenced above. Upon learning of the current investigation into Yarbrough, SA Pickard turned over the case file to me to include the NCMEC cybertips and the content provided with them.

18. On February 4, 2020, I reviewed NCMEC cybertip 51563239. The image provided with the cybertip that was reported by Microsoft Skype is of a minor female's torso, estimated to be under the age of eight (8) year old by lack of body development and features, that can be seen completely nude from her upper thighs to her breast. An adult male with an erect penis is inserting his penis into her vagina. Only the penis, stomach and hand of the adult male can be seen in the images.

19. On February 4, 2020, I reviewed the NCMEC cybertip 51563649 and the content that was provided with the cybertip reported by Microsoft Skype. The video is of an adult male inserting his erect penis into a minor female's vagina. The female is completely nude and can only be seen from mid-thigh to her neck. Written on the minor female's stomach with back marker is "Fuck Me" with an arrow pointing to her vagina. Based on previous investigations, I know this video to be a known series of child pornography that is widely traded.

20. On April 7, 2020, Polk County Police Department Detective Brandy Brady conducted surveillance at the **SUBJECT PREMISES**. Upon locating the residence, Detective Brady obtained photographs of the residence that appear to confirm the residence was still occupied by Yarbrough. On April 29, 2020, I spoke with a relative of Yarbrough at the **SUBJECT PREMISES** who confirmed that Yarbrough lives at the **SUBJECT PREMISES**.

CHARACTERISTICS COMMON TO INDIVIDUALS WITH INTENT TO COLLECT, RECEIVE OR DISTRIBUTE CHILD PORNOGRAPHY

21. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals with intent to view and/or possess, collect, receive, or distribute images of child pornography:

a. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography may receive sexual gratification, stimulation, and

satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children that they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their films, videotapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain photos, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals with intent to view and/or possess, collect, receive, or distribute pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer or other

electronic storage devices. These collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

e. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who would have knowledge about how to access online forums, such as bulletin boards, newsgroups, Internet relay chat or chat rooms are considered more advanced users and therefore more experienced in acquiring and storing a collection of child pornography images.

g. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

22. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers

basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

23. Child pornographers can now transfer printed photographs into a computer-readable format with a scanner. Furthermore, with digital cameras, when the photograph is taken, it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 64 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer. Additionally, almost all cell phones today can record high-resolution photographs and videos.

24. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and

modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

25. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera or a cell phone, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person.

26. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

27. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote

computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

28. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or Internet Service Provider client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CONCLUSION

29. Based on the foregoing information, I respectfully submit that there is probable cause to believe that evidence of violation of Title 18, United States Code, Section 2252(a)(4) (possession of child pornography) is located on the **SUBJECT PREMISES** described in **Attachment A**, and that the evidence, listed in **Attachment B**, is contraband, the fruits of crime, or things otherwise criminally possessed, and/or is property which is or has been used as the means of committing the foregoing offense. I therefore respectfully

request that the attached warrant be issued authorizing the search for and seizure of the items listed in **Attachment B**.